Primer on Privacy
Best Practices for McMaster University

Fazila Nurani, B.A.Sc. (E.Eng.), LL.B., CIPP/C, CISA

Privacy Tune-Up Session
July 22, 2014
Objectives

- In this session you will learn about:
  - The importance of privacy.
  - The privacy law that applies to McMaster University.
  - The 10 fundamental principles of privacy.
  - The risks that poor information handling practices introduce.
  - Practical considerations that will help you meet your privacy obligations.
Primer on Privacy

- What is information privacy?
  - The right to control the collection, use and disclosure of personal information by the University.

- What’s the difference between privacy and confidentiality?
Key Drivers for Getting Privacy Right

- Heightened media attention.
- Heightened public attention.
- Heightened regulator attention.
It’s all about Risk Management

**Information Risks**
- Unauthorized Access
- Unauthorized Disclosure
- Misuse or Unauthorized Use

**Financial Risk**
- Managing the breach
- Notifying individuals

**Confidence Risk**
- Loss of trust

**Legal Risk**
- Damages, fines
The University is governed by the Freedom of Information and Protection of Privacy Act (“FIPPA”).

FIPPA ensures transparency and accountability:
1. Information should be accessible to the public.
2. Personal privacy must be protected.

The Personal Health Information Protection Act (“PHIPA”) governs health professionals working in the University (e.g. psychologists, social workers, etc.).
Role of the Ontario IPC

- Protect the privacy interests of Ontario residents.
- Educate the public and organizations on privacy best practices.
- Interpret privacy laws.
- Investigate and resolve complaints.
- Provide opinions on privacy breaches in the media.
- Help individuals and organizations to recover from breaches.
- www.ipc.on.ca
What is Personal Information (PI)?

- PI is broadly defined in FIPPA to include:
  - Ethnic origin, race, religion, age, sex, marital/family status, etc.
  - Information regarding education, financial, employment, medical, psychiatric or criminal history.
  - Identifying numbers, e.g. SIN, student #.
  - Home address, home telephone number.
  - Personal opinions of, or about, an individual.
  - Personal correspondence.

* Name, position and records about routine work matters is not PI.
## CSA Model Code Principles

<table>
<thead>
<tr>
<th>Accountability</th>
<th>Consent</th>
<th>Limiting Collection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifying Purposes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Limiting Use, Disclosure and Retention</td>
<td>Accuracy</td>
<td>Safeguards</td>
</tr>
<tr>
<td>Openness</td>
<td>Individual Access</td>
<td>Challenging Compliance</td>
</tr>
</tbody>
</table>

CSA = Canadian Standards Association
1. Accountability

The University is responsible for personal information under its control and must ensure accountability for the organization's compliance with the remaining principles.
Accountability in Practice

• All faculty and staff with access to PI are responsible for protecting it.

• The University Secretariat is responsible for ensuring privacy best practice is followed across McMaster’s operations.

• The University Secretary is responsible for managing all escalated privacy issues and can be contacted at univsec@mcmaster.ca

• Privacy assurances must be obtained by third parties who are entrusted with PI.
2. Identifying Purposes

The purposes for which personal information is collected must be identified by the University at or before the time the information is collected.
Identifying Purposes in Practice

• The purposes for which PI is collected must be clear and easy to understand (general notice of collection and notice statements on forms that collect PI).

• No additional uses can be made of the PI without first obtaining consent for such uses.

• You must be able to explain the purposes for which you require PI if asked by the individual providing it.

• Clear purposes are critical for informed consent…
3. Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.
Consent in Practice

Express Consent
- Required when collecting/using/disclosing PI for a purpose other than academics or administration (opt-in consent).

Opt-out Consent
- Should be offered when PI will be used for secondary purposes (the ability to withdraw consent).

Implied Consent
- Relied upon when collecting, using or disclosing PI in accordance with the University’s lawful authority or a consistent purpose.
Examples of Consent Exemptions

• There are contexts in which consent is not required, such as:
  ➢ Collection of PI during an investigation.
  ➢ Use of PI in an emergency situation.
  ➢ Disclosure in response to a valid request from law enforcement, or on compassionate grounds.

• Contact the University Secretariat if you are not sure whether a consent exemption applies.
4. Limiting Collection

The collection of personal information must be limited to that which is necessary for the purposes identified by the University. Information must be collected by fair and lawful means.
Limiting Collection in Practice

• The University only requires the provision of PI that is necessary for fulfilling its academic and administrative purposes.

• Information that is useful but not necessary, should be clearly labeled as optional and only collected with consent.

• Indirect collection must usually be accompanied by consent.

• Never rely on information from non-credible sources.
Personal information must not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information must be retained only as long as necessary for the fulfillment of those purposes.
Limiting Use, Disclosure, Retention in Practice

- PI can only be used/disclosed for an original or consistent purpose.
- Within the University, access to records must be limited on a “need-to-know” basis.
- In most contexts, written consent is needed before disclosing PI outside of the University.
- Be extra cautious to avoid unauthorized disclosures.
- Any temporary notes containing PI must be securely destroyed.
- FIPPA requires institutions to keep all records for a minimum of one year after last use.
Personal information must be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.
• Keeping accurate records is a joint responsibility.
• You rely on students/alumni/employees to provide you with accurate information.
• It is your responsibility to ensure that accurate data is stored in your files.
• An individual has the right to challenge the accuracy or completeness of any information on file (amend or attach a statement of disagreement).
Personal information must be protected by security safeguards (physical, organizational and technological measures) that are appropriate to the sensitivity of the information.
Examples of Organizational Safeguards

Day-to-day practices to protect personal information, such as:

- Frequent reminders to develop a culture of privacy.

- Not leaving personal information unattended and in plain view.

- Mobile device best practices.

- A privacy management framework.

Empowering Organizations to Minimize Privacy Risks
Examples of Physical Safeguards

Personal information is physically safeguarded by:

- Building security.
- Having locked offices, filing cabinets or desks to store personal information.
- Workspace layout that limits unauthorized access.
- Video surveillance cameras.
Examples of Technical Safeguards

Technology is used to protect personal information as follows:

- Using strong passwords for network and systems access.
- System-controlled access rights that depend on one’s job function.
- Employing PINs and other mobile device security features.
- A secure e-mail system, up-to-date firewalls, etc.
8. Openness

The University must make readily available to individuals specific information about its policies and practices relating to the management of personal information.
Openness in Practice

• Transparency is of utmost importance to the University.

• The University is considering the policies and procedures that need to be put in place to support compliance efforts.

• Read and understand McMaster’s Statement on Collection of PI and Protection of Privacy, the FAQs on FIPPA and related material at http://www.mcmaster.ca/univsec/fippa/fippa.cfm

• Direct any questions to the University Secretariat.
Upon request, an individual must be informed of the existence, use, and disclosure of his or her personal information and must be given access to that information. An individual must be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
Individual Access in Practice

• Maintain the individual’s trust and respect their right of access to **any record in the University’s custody or control**.

• The requestor must be authenticated and put their request in writing.

• Access must be provided within 30 days unless:
  • An access exemption applies.
  • It is determined that the request is frivolous or vexatious.
  • The information will soon be published.

• The University’s FOI coordinator handles all formal access requests.
10. Challenging Compliance

An individual must be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the University’s compliance.
Challenging Compliance in Practice

- Take all privacy challenges seriously.
- Inform the University Secretariat of all privacy complaints, regardless of seriousness.
- Complaints must be internally investigated and responded to.
- If an individual making a privacy complaint is not satisfied with the University’s response, they can file a complaint with the Information and Privacy Commissioner of Ontario.
Managing a Privacy Breach

• A privacy breach may be identified internally by a faculty or other staff member, or externally by a student or other member of the public.

• Immediately inform the University Secretariat of a potential or confirmed breach.
Managing a Privacy Breach

- Key steps that the University must take:
  - Respond to the breach
  - Contain the breach
  - Conduct a detailed investigation
  - Determine who needs to be informed about the incident, internally and externally
  - Take the necessary steps to prevent a similar breach from occurring
• Privacy must be balanced with other interests (e.g. security and safety).

• Respond quickly and with transparency to privacy inquiries.

• Courts are not rubber-stamping decisions of the privacy commissioners.

• To date, privacy non-compliance has been costly from a reputation perspective in Canada, but not costly from a monetary point of view.
“The fact that the Respondent has never denied having committed the errors is commendable…. the Respondent has apologized to the Applicant on numerous occasions …. It may be, as alleged by the Applicant, that the Respondent should have put these measures in place before the error occurred. Nobody should be held to a standard of perfection, and the Respondent already had a detailed protocol before the occurrence of what can only be considered as a human error.”

*Townsend v. Sun Life Financial*, 2012 FC 550
“The fact that the Respondent has never denied having committed the errors is commendable. … the Respondent has apologized … be, as alleged by the Applicant, that the Respondent should have put these measures in place before the error occurred. Nobody should be held
• Tsige accessed Jones’ privacy financial records without work-related purposes on several occasions.
• Ontario Court of Appeal released its decision in Jones v. Tsige recognizing a tort of invasion of privacy (“intrusion upon seclusion”).
• Individuals now have an avenue to sue others for invading their privacy.
• The court set an upper limit of $20,000 on such a claim.
• The three elements of the cause of action:
  ➢ An intentional act;
  ➢ An intrusion upon the privacy of another; and
  ➢ The act is highly offensive to a reasonable person.
Inappropriate access by clerks of the health authorities:
- Eastern Health – 46 records
- Western Health – 1043 records

Patients claiming loss of income and mental anguish have been compensated in a class action lawsuit.
Hopkins v. Kay (2014, ONSC)

- Plaintiffs allege the defendants wrongfully accessed the private medical information of 280 patients without their consent.
- Claim based on tort of “intrusion upon seclusion”.
- Motion to strike based on allegation that the tort is precluded by Ontario’s PHIPA.
- Motion dismissed with costs of $24,000.
- Tort claim can proceed even if statutory privacy right exists.

• Confirmation that employees may have a **reasonable expectation of privacy** in the information contained on their work computers, if personal use is permitted or reasonably expected.

• Workplace policies and the organization’s ownership of the laptop diminished the expectation of privacy, but did not eliminate it.

• Infringement upon Cole’s right to be free from unreasonable search and seizure – receipt of the computer did not afford the police warrantless access to the personal information stored on it.
IPC Orders - Invasion of Privacy

- PO-3329:
  - The appellant was the subject of a large number of requests under the Act made to the University of Ottawa. He requested records relating to those requests.
  - Identities of requesters constitutes their PI – the requests were not made in some professional or business capacity, and would reveal other PI about the individual.

- PO-3298:
  - The appellant made a request for records related to his performance as a medical resident at the University of Ottawa.
  - PI withheld relates to employment and educational history of university and hospital employees as well as other medical residents.
Loss of Information on Mobile Devices

- February 2014: Edmonton woman launches $11-million class action lawsuit against Medicentres over a stolen laptop that contained the health information of 620,000 Albertans.

- August 2013: Investment Industry Regulatory Organization loses the financial information of 52,000 brokerage firm clients (employee loses “portable device”).

- January 2013: HRSDC lost an unencrypted hard drive containing personal information of 583,000 people who had a Canada Student Loan between 2000 and 2006.

- July 2012: Elections Ontario lost 2 unencrypted memory sticks containing data on 2.4 million voters (names, home addresses, dates of birth, gender, voting history).
Where Have we Come on Privacy?

- First Wave:
  - Privacy = “Right to be Let Alone”

- Second Wave:
  - Privacy = “Right to Respect for Private and Family Life”

- Third Wave:
  - Privacy = “Control over Your Personal Information”

- Fourth Wave?
  - Privacy = Transparency…the right to understand HOW one’s “personal information” is being used.
Empowering Organizations to Minimize Privacy Risks

Getting Privacy Right

• It takes educated **people**, strong **technology** and sound **processes** to minimize the risk of a privacy breach.
Questions?